



HOMELAND SECURITY COMMITTEE

Statement of Subcommittee Chairman Scott Perry (R-PA) Oversight and Management Efficiency Subcommittee

“Examining DHS’ Efforts to Strengthen its Cybersecurity Workforce”

March 7, 2018

Remarks as Prepared

Good afternoon. I would like to thank Chairman Ratcliffe for holding this hearing today and including the Oversight and Management Efficiency Subcommittee in this very important and timely discussion on the Department of Homeland Security’s efforts to strengthen its cybersecurity workforce.

In today’s world, our nation and its critical infrastructure face an increasingly diverse and sophisticated array of cybersecurity threats from both state and non-state actors. Adversaries across the globe have invested heavily in building out cyber capabilities and have demonstrated an increasing capacity to successfully execute cyber-attacks against the U.S. and our allies.

As the lead civilian agency for securing the nation’s public and private critical infrastructure, which is dependent on IT systems and electronic data, the Department of Homeland Security (DHS) and its workforce play a critical role in protecting the nation’s cyberspace. Given this role, data continuing to show cyber personnel shortages at DHS must remain a top concern for both DHS and this Committee. Demand for cyber-related positions continues to outpace the number of individuals qualified to fill them and agencies like DHS must compete with the private sector in attracting highly skilled cyber workers.

To address these challenges, this Committee has passed several pieces of legislation in recent years that were signed into law providing DHS with additional hiring authorities to better recruit and retain a qualified cyber workforce. The Homeland Security Cybersecurity Workforce Assessment Act, enacted into law as part of the Border Patrol Agent Pay Reform Act of 2014 (Public Law 113-277), required DHS to survey its workforce and identify, categorize, and code all vacant and non-vacant cybersecurity positions. The act aimed to help DHS assess its current cyber workforce in order to identify skills gaps and critical needs, and improve strategic workforce planning to more effectively recruit, hire, train, and retain cyber personnel.

Unfortunately, according to a recent U.S. Government and Accountability Office (GAO) report, DHS has failed to implement the actions required by this act in a timely, accurate, or complete manner. GAO audited six components and found that the Department has not met any of the deadlines established by the act. Two-and-a-half years after the statutory deadline to identify and code positions, three of the six components studied still have not identified all of their cyber positions

and, as of August 2017, the Department has only assigned employment codes to 79% of its identified cyber positions. Further, while DHS has identified cyber workforce capacity and capability gaps, it has not submitted to Congress and the U.S. Office of Personnel Management (OPM) required reports on critical needs aligned with the National Initiative for Cybersecurity Education's National Cybersecurity Workforce Framework.

Congress has acted to provide DHS with the tools to help meet the workforce needs demanded by the current cyber threat environment. The Department's failure to utilize these tools is unacceptable. Bureaucratic delays in hiring the personnel needed to secure our nation's cyberspace are detrimental to our national security.

Sadly, the failure to properly implement cyber-related hiring authorities is emblematic of the systemic hiring issues continuing to plague the Department. A management report released by DHS's Office of the Inspector General last fall aptly summarized that the Department and its components continue to encounter significant hiring difficulties related to long hire times and a lack of human resources staff, automated systems, and processes to determine needed staff. Just last week, the Oversight and Management Efficiency Subcommittee heard testimony on the ineffectiveness and delays associated with the Department's fitness determination process, an integral part of the contract workforce's onboarding process.

These problems are especially alarming, given the significant responsibilities facing DHS as it prepares to meet cyber workforce needs and undertake the border security-related hiring surge mandated by the President.

I want to thank our panel for testifying this afternoon and I look forward to hearing an update on the Department's implementation of Public Law 113-277's requirements, as well as how DHS's Management Directorate is working with components to improve hiring processes.

Thank you and I yield back the balance of my time.

###